required to designate a senior officer or employee to serve as a point of contact?[45] Presumably this designated list and point of contact information would be made available to the Commission *via* its proposed rule 64.1705 or to law enforcement, although the Commission never specifically states that such would be the case.

Designated employees would be required to create records (see discussion below on Recordkeeping), independent of those routine notations that non-designated employees might memorialize, assuring the effective supervision of work performed by non-designated employees. Non-designated employees "would be permitted to effectuate certain legal surveillance work, provided they do such work unknowingly, as part of their routine work assignments."[46]

It is not clear from the Commission's discussion in the NPRM what the specific regulatory purpose would be of requiring specific employee designations in a carrier's internal practices and procedures or requiring a "statement" that only designated employees are permitted to assist law enforcement. For that reason, U S WEST opposes the Commission's proposal that such requirement be incorporated into a formal rule.

First, specific employees are probably already designated to deal with law enforcement in many companies, as a matter of both administrative and operational

---

[45] Id. ¶ 33. The list of "designated employees" would also include individually-identifiably-related information such as date and place of birth, social security number, official title, and contact telephone numbers and pager numbers. Id.

[46] Id. ¶ 30.

efficiency.[47] Second, a "statement" in a carrier practice incorporating such corporate decisions is not "necessary" to effectuate or ensure compliance with Section 229 or Section 105 of CALEA. Third, there is nothing in the NPRM discussion that suggests that the identifications of the designated employees be made available either to the Commission or law enforcement.[48] While U S WEST supports the absence of such a requirement, it renders the fundamental basis for the requirement (i.e., the fact of designation) illusory.

For these reasons, the Commission should not promulgate a formal rule on the need for a company to designate certain employees to interact with law enforcement. While the Commission might determine that a simple "statement" obligation is appropriate with respect to a Guideline, should the Commission be inclined to go beyond that -- into the realm of disclosure of the designated employees -- it should consider the effect on corporate operations (including the

---

[47] Internally, U S WEST incorporates the notions of designated versus non-designated employees in its daily operations. The Work Group supervisor, the supervisor's manager, the manager's director and an attorney within the Law Department providing legal advice to the Group, maintain oversight responsibility for cooperating with law enforcement and implementing lawful interceptions.

When U S WEST receives service of a valid court order for interception, the order itself generally contains a limitation on who the information can be shared with. U S WEST always complies with the requirements of the court order, sharing the information only among the Security employees with a "need to know" and with the sponsoring law enforcement agency or order-issuing court.

[48] At U S WEST, our current security policies and procedures incorporate the provision of relevant information to law enforcement. Such information includes, as appropriate, a list of designated employees with respect to FISA activities (which list actually reflects those U S WEST employees who have undergone a National Security Clearance and are, therefore, capable of handling FISA requests), as well as an identification of appropriate work units and telephone numbers to be contacted with respect to particular types of interceptions.

need to make amendments to the list to reflect changes in personnel, etc.), the privacy interests of the designated employees, as well as whether any material benefit is realized by regulators or law enforcement from the availability of such a list.

b. Non-Designated Employees

The Commission makes a specific proposal that carriers include in their practices a requirement that non-designated employees be permitted to act as agents in the effectuation of legal surveillance only if they do so "unknowingly, as part of their routine work assignments."[49] The Commission's requirement of "unknowing" participation may overstate the realities of the process. The Commission would be better served proposing (preferably by Guideline) that non-designated employees not be informed of the specifics of the legal surveillance and be trained to avoid the memorialization of the specifics associated with the effectuation of lawful interceptions. Since this is undoubtedly a current carrier practice in many instances, due to the legacy of the AT&T black binders practices and procedures, U S WEST believes that such a Guideline would be easily achievable.

While U S WEST cannot speak for all corporate organizations, we can advise as to our current practices and policies. While these practices incorporate a policy of anonymity and non-revealing note memorialization, they would not necessarily reflect "unknowing" activity by employees.

---

[49] NPRM ¶ 30.

At U S WEST, non-Security employees (i.e., non-designated employees) are never advised of the specifics of a court order's requirements. Furthermore, every effort is taken to involve such employees only in ministerial activities necessary to effectuate the specifics of the court order. However, non-ministerial employees are aware when they are engaging in activities associated with the Security Department. In this respect, their conduct is embued with some element of "knowledge" of a connection with law enforcement.

With respect to our business office employees, their interaction with interceptions begins when the Security Work Group initiates a service order under a fictitious billing account (associated with the law enforcement agency involved in the interception). The business office processes the service order from the Work Group and assigns a service ticket to the appropriate network personnel. The business office personnel will know of the involvement of the Security Work Group and will note the account that Security is involved in the order activity.

The network personnel are responsible for installing necessary equipment and/or performing necessary switch translations to effectuate the interception. These personnel are aware of the actual target of the interception only by telephone number. They will also record "Security involvement" in their ministerial note logs, but will not record the specifics of the interception (i.e., whether the interception was accomplished *via* a trap-and-trace device or a pen register).

The Security Work Group maintains detailed records on each court order interception processed. The Security Department records include the names of the business office and network individuals who processed the work.

Whether this type of process would be included in the Commission's proposed procedure requiring "unknowing" routine activity by non-designated employees is not clear. What is clear is that the process employed by U S WEST is a sound one from a business perspective, does not compromise individual expectations of privacy and promotes the efficient administration of lawful surveillance. The Commission should promote no Guideline or rule that would prohibit the current practice.

4. The Need For Officer/Employee Affidavits

The Commission proposes requiring that a carrier's security policies and procedures require each employee and officer who will knowingly engage in an interception activity to sign an affidavit regarding a variety of items.[50] Alternatively, the Commission suggests that a single affidavit (from an officer or an employee) might suffice.[51]

U S WEST opposes the notion of internal affidavits in its entirety. U S WEST processes around 1,500 court orders a year. The Commission's proposal

[50] NPRM ¶ 31. The items would include the telephone number or the circuit identification numbers involved; the name of each employee and officer who effected the interception and possessed information about its existence and their respective position within the carrier; the start date and time of interception; the stop date and time of interception; the type of interception; a copy or description of the written authorization for the employee and officer to participate in interception activity; a statement that the employee or officer will not disclose information about the interception to any person not properly authorized by statute or court order. Id.

[51] Id.

would require, at a minimum, 1,500 employee affidavits and a potential maximum of 3,000. While there may be only minimal costs in having an individual sign a "form" affidavit with respect to the effectuation of each interception request, the administrative burden associated with making sure that each employee, in fact, follows through on the requirement could be significant.[52] An entire "affidavit administration" component would need to be added to existing carrier practices. While the cost might be minimal, the benefit to be achieved from such a requirement is not at all evident, from either a law enforcement, regulatory or operational perspective. Thus, the Commission should reject the notion of internal affidavits.

Should any type of "affidavit" approach be appropriate with respect to carrier operations and practices, at most it should be an external type of affidavit, such as is incorporated into the ONA regulatory structure, i.e., where a responsible office of the corporation swears that compliance with all Commission rules and requirements is occurring.[53]

---

[52] Following through, of course, requires that if it were determined that an employee had not signed the requisite affidavit that appropriate follow-up actions (including potential discipline) were pursued. Thus, the activity can become resource intense and costly. Furthermore, should the Commission determine to require carriers to self-report violations of internal carrier practices (see discussion below at 44-46), carriers would be obliged to engage in the further administrative burden of reporting the failure to execute the affidavit to the Commission.

[53] See In the Matter of Amendment to Sections 64.702 of the Commission's Rules and Regulations (Third Computer Inquiry), 3 FCC Rcd. 1150, 1160 ¶ 76 (1988).

5. Recordkeeping And Record Retention Proposals

In an effort to establish rules deemed "necessary" under Section 229(b)(1)(B) (which requires that carriers establish policies and procedures to secure and maintain records associated with any interception, be it lawful or unlawful), the Commission proposes requiring carriers to maintain detailed records, including seven specific items.[54]

In addition to the specifics of the record keeping itself, the Commission proposes that carriers be required to create such records contemporaneous with each interception or no later than 48 hours after such interception. Furthermore, carriers would be required to retain such records for a minimum of 10 years, a time frame which the Commission claims is currently incorporated into 18 U.S.C. § 2518(8)(a).[55]

U S WEST opposes the detailed recordkeeping and retention requirements proposed by the Commission, particularly those associated with recordkeeping of "times" (as opposed to dates)[56] and the proposed record retention obligations. Once

---

[54] NPRM ¶ 32. The items include: the telephone number or the circuit identification numbers involved; the name of each employee and officer who effected the interception and possessed information about its existence and their respective position within the carrier; the start date and time of interception; the stop date and time of interception; the type of interception; a copy or description of the written authorization for the employee and officer to participate in interception activity; a statement that the employee or officer will not disclose information about the interception to any person not properly authorized by statute or court order. Id.

[55] Id.

[56] U S WEST currently records the start and stop date of interceptions, not the time. From our experience, the latter is not a relevant factor either in the institution of a lawful interception or its cessation. For this reason, regardless of whether the

again, the Commission's proposal goes beyond reasoned regulatory protocol and significantly interferes with business management prerogatives. Such is not necessary from the perspective of statutory compliance, reasoned regulatory policy or the public interest.

Carriers undoubtedly already incorporate recordkeeping obligations of employees into their internal practices and policies. For example, U S WEST already records the vast majority of the information which the Commission proposes be codified in a formal Commission rule.[57] Thus, whether required by rule or *via* a "safe harbor"-type approach, U S WEST's current practices/policies would comport with the desires of the Commission.

However, with respect to the reasonable record retention obligations that might be incorporated into any Commission Guideline or rule, the Commission has wrongly interpreted the requirements of Section 2518(8)(a). Neither U S WEST nor other carriers, we believe, would be able to comply or "certify" compliance with a ten-year retention period.[58] However, U S WEST does not believe such obligation to be supported by current legal requirements, nor appropriate as a matter of business practice.

Commission pursues a Guideline or rule approach to its proposed requirements, the obligation to record and retain start/stop "times" should be eliminated.

[57] As noted above in note 56, U S WEST does not currently record the start/stop "times" associated with interceptions.

[58] Currently, pursuant to corporate retention policies, U S WEST possesses its detailed interception records for three years.

The language of Section 2518(8)(a) does not support the Commission's conclusion that carriers are required to retain interception records for ten years. The Section cited by the Commission pertains to record retention obligations imposed on law enforcement -- not carriers. Such is evident from the language of the Section itself, which states in pertinent part:

> ***[c]ustody*** of the ***recordings*** shall be wherever the judge orders. They shall not be destroyed except upon an order of the issuing or denying judge and in any event shall be kept for ten years.[59]

The Section discusses the "*custody* of the *recordings*." U S WEST never possesses custody of the interception recordings. Rather, U S WEST installs devices and/or translates switch software which allows the interception *recording* to be delivered directly to and only to law enforcement. U S WEST neither listens to nor monitors the effected interception. Nor does it keep a copy of the interception or the recording. In this respect, U S WEST does not deem its current practices as materially different from other carriers.

Section 2518(a) imposes a ten-year retention burden on law enforcement agencies who presumably possess custody of the recordings, as evidence in their endeavor to pursue and prosecute criminals. The record retention obligation statutorily imposed on law enforcement should not be extended to carriers. Rather, the Commission should allow carriers to continue to follow industry custom, practice and standards for their internal recordkeeping requirements.

---

[59] 18 U.S.C. § 2518(8)(a) (emphasis added).

6. Information Provided To Law Enforcement

The Commission inquires as to the "nature" of information that carriers should be required to provide law enforcement personnel with respect to the processing of interceptions.[60]

In line with U S WEST's other comments, it must be obvious that U S WEST would oppose any type of mandate regarding the types of information carriers must provide to law enforcement. The end goal is to provide law enforcement with sufficient, and appropriate, information to allow them to efficiently interact with carriers and those work groups or employees whose primary job responsibilities are to facilitate and implement lawful process regarding interceptions.

Furthermore, as with other of the Commission's proposals, U S WEST believes that the substantive goal which the Commission hopes to achieve is already met by many carrier internal practices and procedures. For example, U S WEST and law enforcement in U S WEST's 14-state territory have established the Work Group as the point of contact for law enforcement agencies seeking to serve court orders for lawful interceptions. U S WEST also operates a 24-hour emergency center for law enforcement emergencies and 911 centers. These around-the-clock operations afford law enforcement a point of contact after normal business hours.

Moreover, U S WEST published and makes available a Law Enforcement Agency Guide. U S WEST developed this Guide to assist law enforcement agencies

---

[60] Id.

in understanding the Work Group's roles and responsibilities and law enforcement agencies' roles and responsibilities in effectuating lawful interceptions. The Guide outlines policies and procedures for law enforcement to follow when requesting U S WEST assistance for lawful interceptions. The Guide provides contact telephone numbers for those work units who specialize in processing particular types of interception requests.

It is obvious that at least some companies already have practices and procedures in place that facilitate meaningful communication and cooperation between carriers and law enforcement. The Commission should not mandate a particular type of medium or message with respect to that coordination.

IV. FORMAL COMMISSION REVIEW OF CARRIER POLICIES SHOULD BE DRIVEN BY THE SUBSTANCE OF THOSE POLICIES NOT BY CARRIER REVENUES

As discussed above, the Commission should not -- by way of formal rule -- outline or prescribe the details of any carrier's internal practices or policies with respect to cooperation with law enforcement. Rather, an incentive approach should be pursued. Such an approach would, undoubtedly, result in the vast majority of carrier practices/policies conforming to what the Commission viewed as an ideal model, without inappropriate Commission micromanagement of a carrier's business operations.

The Commission could outline certain elements that it desires to see in a carrier internal practice/policy. Such outline might include many of the Commission's tentative proposals (without -- it is hoped -- the ten-year retention obligation derived at through an erroneous statutory interpretation). If a carrier's

internal practices or policies incorporated those elements which the Commission deemed ideal, the Commission could circumscribe its review process, such that only an officer certification that the carrier's practices/policies met all the Commission's desired elements would be necessary under Section 229(c).

Carriers whose practices or policies did not currently comport with the Commission's "Guidelines" would have a choice. Either they could modify their own practices or policies or they could submit them for Commission review, explaining any deviations from the Commission's guidelines. At that point, the Commission could either determine that the deviation was appropriate or could require a modification to the carrier plan.

An additional benefit of this type of approach is that it would manage the carrier policy/practice submissions to the Commission in a manner that was more substantively meaningful than carrier revenues. There is nothing inherently meaningful about carrier revenues that suggests that those carriers with larger revenues (i.e., large incumbent carriers, either local exchange carriers ("LEC") or interexchange carriers ("IXC")) will benefit from substantive Commission review of their internal practices/policies or that the Commission will play a meaningful editorial or review role in the process. Given that the larger carriers are more likely to have been participating with law enforcement historically,[61] their

[61] As the Commission observed in a predictive remark, "It is conceivable that many of the small and rural telecommunications carriers subject to CALEA requirements may never be asked to conduct electronic surveillance." NPRM ¶ 34. This remark is no less true of many of the new entrants that might not be "small" by either corporate revenue or affiliation but might be small with respect to the number of access lines served.

practices/policies are probably already more sophisticated and more detailed. Little would be accomplished by a formal Commission review of such policies that could not be accomplished by an officer certification.

If carrier size alone were a relevant factor in determining the need for carrier submissions of practices and policies, logic suggests that Commission review should be reserved for the practices and policies of the smaller and newer carriers. It is those carriers that probably do not have daily encounters with law enforcement and need the discipline of detailed written practices and procedures to guide them lawfully through the process. And, contrary to the suggestion of the Commission, at least with respect to the creation of practices and procedures, the "resources" necessary to create such practices and procedures is not so burdensome that smaller telecommunications carriers are less able to create such documents than larger carriers.[62]

U S WEST's proposal advances the objectives of CALEA and reasoned regulatory policy. Rather than attempting to differentiate carriers by factors that are not material to their advancement of legislative objectives (and may, in fact, operate contrary to those objectives), U S WEST's proposal allows the Commission to craft the differentiation by substance. If a carrier practice/policy includes certain items, it need not be submitted *in toto*. Rather, an officer affidavit that the

[62] Compare NPRM ¶ 36 (suggesting that smaller and newer telecommunications carriers may be less able to meet CALEA requirements because they lack the resources of larger telecommunications carriers).

practices/policies incorporate the suggested items would be all that was necessary.[63] Those carriers -- large or small -- that chose to craft practices or policies that fail to include all the elements desired by the Commission would be required to submit the entirety of the practice/policy for review -- with a possible requirement that the practice/policy be modified.

V. RATHER THAN APPROACH THE MATTER FROM THE ABSTRACT PERSPECTIVE OF DEFINING THE "STANDARD" NECESSARY TO MEET EITHER SECTION 107 OR 109 OF CALEA, THE COMMISSION SHOULD DECLARE THAT COMPLIANCE WITH CALEA'S REQUIREMENTS IS NOT NOW "REASONABLY ACHIEVABLE" AND THAT COMPLIANCE WILL NOT BE REASONABLY ACHIEVABLE UNTIL THE PERTINENT CAPABILITIES HAVE BEEN IMPLEMENTED INDUSTRYWIDE IN EQUIPMENT GENERALLY AVAILABLE TO CARRIERS IN THE MARKETPLACE

CALEA calls on the Commission, on petition by a carrier or other interested person, to determine whether compliance with the statute's capability requirements is "reasonably achievable." Although a specific determination of whether the standard of "reasonably achievable" has been met does not need to occur until the point in time at which a petition is filed, the Commission requests comment on the "specific factors contained in Section 109(b)(1), (a) through (j)," as well as other factors that should bear on the ultimate determination of whether CALEA compliance is reasonably achievable.[64] Along the same lines, the Commission requests comment on what factors it should consider with respect to an extension of time petition under Section 107, which also requires a consideration of whether

[63] See note 50, supra.

[64] NPRM ¶ 48.

CALEA compliance is "reasonably achievable."[65]

In the NPRM, the Commission treats the issue of "reasonably achievable" status as something of an intellectual discussion of relevant statutory criteria. That is, the Commission has a statute allowing for certain actions (i.e., the filing of petitions or requests for extension of time), and the Commission is inquiring as to the appropriate "standard" to be applied should one of those actions or events occur.

While the Commission's approach to addressing the issue of "reasonably achievable" status is understandable from a certain perspective, the Commission should move beyond addressing this issue in the abstract. While the Commission has not yet been the recipient of a petition under Section 109 or a request for extension under Section 107, the standard adopted as to the meaning of "reasonably achievable" under either Section should be dispositive with respect to current carrier obligations and CALEA compliance. The fact is, under either Section 107 or 109, current CALEA compliance is not reasonably achievable. The Commission should so state, thereby alleviating confusion by those parties affected by CALEA implementation mandates and forestalling future requests for enforcement.

---

[65] Id. ¶ 49. Under Section 107(c) of CALEA, the Commission may grant one or more extensions of the deadline for compliance with respect to equipment installed or deployed before the effective date of Section 103 (currently October 25, 1998), if the Commission determines that compliance "is not reasonably achievable through application of technology available within the compliance period."

Because Section 107(c) explicitly provides for "one or more" extensions, the Commission's statement that it may grant an extension only until October 24, 2000 (NPRM ¶ 49) is incorrect. Although the first extension granted to a carrier can last no later than October 24, 2000, the Commission has authority to grant further extensions beyond that date.

With respect to interpreting the "reasonably achievable" requirements of both Sections 107 and 109, the focus of the determination should be on whether the technology necessary to implement the pertinent capability requirement is generally available in equipment and associated software that carriers may procure.[66] In the case of a petition for extension of the compliance date, compliance is not reasonably achievable unless the particular manufacturer(s) from which a carrier has purchased the pertinent equipment has implemented the technology necessary to achieve compliance in equipment or software available for sale to the carrier.[67] In the case of equipment installed or deployed after January 1, 1995, compliance is not reasonably achievable unless, at minimum, the requisite technology has been implemented in equipment available on an industrywide basis.

A. "Reasonably Achievable" Under Section 107(c)

Under Section 107(c), the statute itself requires the Commission to determine whether compliance is "reasonably achievable through application of technology available within the compliance period."[68] Thus, the focus of the Commission's inquiry must be on what technology has been available to the carrier during the

---

[66] The Commission proposes to make both the Section 107 and Section 109 "reasonably achievable" determinations on the basis of the factors listed in Section 109(b) (NPRM ¶¶ 48, 50). While it is correct that the two inquiries are similar, U S WEST does not agree that the inquiry under Section 107 should be made simply by importing the criteria listed in Section 109, as suggested by the Commission.

[67] Of course, if the marketplace produces equipment that can provide all the required capabilities for all manufacturers' products, then compliance could be deemed reasonably achievable for all carriers.

[68] 47 U.S.C. § 1006(c)(2) (emphasis added).

time before the compliance deadline. Such an approach is entirely sensible -- compliance cannot be "reasonably achievable" if the technology necessary to achieve compliance is not available to the carrier.

The fact that the pertinent technology is available in a research lab, or is still being developed, does not make compliance achievable for a carrier. Rather, a carrier can reasonably achieve compliance only if the necessary technology has been finally implemented in telecommunications equipment that is currently available for purchase in the marketplace. Otherwise, the carrier has no practical way of incorporating the technology into its network.

Furthermore, a carrier's compliance is not reasonably achievable unless the manufacturer of the carrier's pertinent equipment (or of compatible equipment) has implemented technology on a generic basis that permits compliance with a particular capability requirement. Two reasons compel this conclusion. First, as the Commission is well aware, because the equipment of different manufacturers is neither compatible nor substitutable, one manufacturer's solution for providing CALEA capabilities cannot be used with the equipment of another. If a carrier's network contains switches only from manufacturers A and B, for example, compliance is not reasonably achievable for that carrier if manufacturer C -- but not A and B -- has implemented technology that would allow a particular interception capability. Second, a requirement of generic availability is necessary in order to ensure that carriers and manufacturers alike will benefit from economies of scale that can be achieved when new capabilities are developed as standard features provided for all a manufacturer's equipment.

B. "Reasonably Achievable" Under Section 109(b)

The Commission should focus on similar issues in determining whether, as a threshold matter, compliance may be reasonably achievable for purposes of Section 109(b). Under Section 109(b), the Commission must determine whether compliance is "reasonably achievable" with respect to equipment installed or deployed after January 1, 1995.[69] In making this determination, the Commission must consider the statutory factors enumerated in the NPRM to determine whether "compliance would impose significant difficulty or expense on the carrier or on the users of the carrier's systems."[70]

Clearly, if the needed technology is not implemented in equipment available to a carrier, compliance would "impose significant difficulty or expense on the carrier."[71] More generally, it would make little sense for the Commission to find that compliance with a particular capability is reasonably achievable if a court could not even issue an enforcement order requiring a carrier to provide that capability. Yet a court cannot issue an enforcement order unless compliance would

---

[69] Id. § 1008(b).

[70] NPRM ¶ 45. If, in response to a petition under 47 U.S.C. § 1008(b)(1), the Commission finds that a carrier's compliance is not reasonably achievable, the carrier is deemed to be in compliance unless the Attorney General agrees to reimburse the carrier for the costs of making compliance reasonably achievable. 47 U.S.C. § 1008(b)(2).

CALEA's enforcement provision states that a court may not require a carrier to provide a capability if the Commission has determined (pursuant to Section 109(b)) that compliance is not reasonably achievable, and the Attorney General has not agreed to reimburse the carrier for the costs to make compliance reasonably achievable. Id. § 1007(c)(2).

[71] Id. § 1008(b)(1).

be reasonably achievable "through the application of available technology."[72]

Furthermore, unlike the reasonably-achievable inquiry undertaken pursuant to a petition to extend the compliance deadline, the inquiry under Section 109(b) must consider the effects on competition in the telecommunications marketplace.[73] This focus requires that compliance not be deemed reasonably achievable unless the requisite technology is available on an industrywide basis. Otherwise, if the necessary technology were available from manufacturers A and B but not manufacturer C, then carriers that use equipment from A and B would have to bear the costs of providing the CALEA capability, while carriers that use equipment from C would either not have to provide the capability or would be reimbursed by the government for doing so. In either case, the result would be a distortion of the competitive marketplace, because some carriers' costs (and therefore rates) would be higher than others.

This focus on the availability of technology, and in particular whether the technology is available on an industrywide basis, is entirely consistent with the factors enumerated in Section 109(b) to guide the reasonably-achievable inquiry. If

---

[72] Id. § 1007(a)(2). A Commission determination that compliance with a particular requirement is reasonably achievable even though the necessary technology is unavailable could create a situation in which the carrier is obligated to provide and pay for a particular capability requirement, according to Commission mandates, while neither the courts nor any other entity could enforce this alleged obligation. Congress surely did not intend to create such a result. Thus, at minimum, the Commission should find that compliance is not reasonably achievable unless the requisite technology is implemented and available to carriers.

[73] Id. § 1008(b)(1)(I); Cong. Rec. H10781 (daily ed. Oct. 4, 1994) (reasonably achievable inquiry under 47 U.S.C. § 1008 must ensure that "the goal of encouraging competition in all forms of telecommunications is not undermined").

the technology needed to achieve compliance has not been implemented in equipment available to the entire industry, many of the statutory factors would strongly support -- and their combination would compel -- a finding that compliance is not reasonably achievable in any real sense.

For example,

- A carrier which did not have access in the marketplace to equipment with the necessary technology would incur significant costs in developing and implementing the technology. As a result, the "cost of the equipment . . . at issue" would increase (see CALEA Section 109(b)(1)(E)). Additionally, because the Attorney General would not be obligated to reimburse the carrier for these costs, if the Commission found compliance to be reasonably achievable, the carrier would have to apply for rate increases to recoup its costs (see CALEA Section 109(b)(1)(B)).

- The fact that the needed technology would be developed not on an industrywide basis but by individual carriers engaging in overlapping research and reaching varying technical solutions would result in compliance not being achieved by "cost-effective methods" (see CALEA Section 109(b)(1)(D)).

- Having carriers find individual technical solutions and then grafting them on equipment bought from manufacturers rather than having the manufacturers implementing the needed technology in their own equipment could well increase the chance of errors and problems in the operation of the network (see CALEA Section 109(b)(1)(F)).

- If carriers must devote their resources to designing and implementing technologies needed for compliance with CALEA because such technologies are not generally available, they will have fewer resources to devote to developing "new technologies and services to the public" (see CALEA Section 109(b)(1)(G)).

Thus, before determining that compliance with a particular capability requirement is reasonably achievable, the Commission should find that the requisite technology

must have been implemented in equipment available to carriers on an industrywide basis.[74]

In making the reasonably-achievable determination at this stage, the Commission should bear in mind that a finding that compliance is not reasonably achievable does not mean that compliance will not occur. Such a finding only shifts the costs of making compliance reasonably achievable from the carriers and their customers to the government. Thus, if the government deems a particular capability to be of great importance to national security (one of the statutory factors), it can still pay for the implementation of that capability, even if the Commission finds that compliance is not reasonably achievable.

VI. MISCELLANEOUS MATTERS ADDRESSED BY THE COMMISSION

The Commission requests comment on the extent to which the duty created by Section 105 of CALEA -- to ensure that interceptions are lawfully authorized and in accordance with Commission regulations -- might extend vicarious criminal and civil liability to a carrier, if the carrier's employees are convicted of intercepting communications illegally.[75] The Commission also requests comment on whether a rule that requires carriers to report illegal wiretaps and compromises of confidentiality would modify or mitigate a carrier's liability under 18 U.S.C. §§ 2511

---

[74] Even if this threshold requirement is satisfied, the Commission may find that compliance is nonetheless not reasonably achievable based on the factors enumerated in the statute. The Commission might find, for example, that the cost of compliance outweighs any benefit.

[75] NPRM ¶ 27.

and 2520.[76]

Nothing in the statute suggests that a carrier's duties under CALEA should affect its liability under other statutes such as 18 U.S.C. §§ 2511 and 2520. Certainly, Section 105 itself does not extend a carrier's vicarious liability beyond whatever scope it would otherwise have. As employers, carriers are subject to the possibility of vicarious liability for misdeeds by their employees, and Section 105 of CALEA merely reiterates the duty of carriers to take reasonable measures to prevent such misdeeds.

However, the Commission's rules implementing Section 105 could expand the scope of carriers' vicarious liability. In considering whether to impose such liability on a carrier under 18 U.S.C. §§ 2511 or 2520, a court could take into account the carrier's compliance with Commission rules. Therefore, the Commission could inadvertently expand the risk of such liability by establishing regulatory requirements that are more detailed or rigid than necessary to achieve the purposes of Section 105. For this reason, in addition to those set forth in Section III of these comments, the Commission should adopt a flexible regulatory approach in promulgating rules under Section 105. The Commission also should explicitly discourage the potential expansion of vicarious liability by stating that its rules are not intended to enlarge the scope of an employer's liability under separate statutory provisions.

Similarly, the Commission should not require carriers to report illegal

[76] Id.

wiretaps and compromises of confidentiality.[77] CALEA itself does not suggest any such requirement. In the absence of an explicit statutory requirement, the Commission should not take an action that might expand criminal and civil liability without having clear evidence that doing so would substantially promote the goals of CALEA. Such evidence is utterly lacking here; indeed, U S WEST is not aware of any carrier violations of 18 U.S.C. § 2511.

What is more, a mandatory self-reporting rule is unnecessary. Carriers currently have significant incentives to report unlawful interceptions to both the relevant law enforcement agency and the Commission itself. In deciding whether to prosecute a corporation for its employee's unlawful interception, law enforcement would normally consider whether the corporation voluntarily, promptly, and fully reported the employee's conduct. Similarly, a court would unquestionably consider that fact as a mitigating factor in imposing any sentence on such a corporation. In addition, the Commission itself has a policy of reducing the sanctions it imposes for violations of its rules where the entity subject to those rules makes such a report.[78]

Carriers also have strong incentives to behave responsibly both before and after unlawful interceptions. Regardless of the Commission's rules, carriers already face the possibility of substantial fines for unlawful interceptions carried out by their employees.[79] Under 18 U.S.C. § 3572, those fines may be reduced based on

---

[77] See id.

[78] See, e.g., Hospers Telephone Exchange, Inc., Memorandum Opinion and Order, 10 FCC Rcd. 12001 (1995); Pass Word, Inc., Order, 76 F.C.C.2d 465, 517 (1980), aff'd sub nom. Pass Word, Inc. v. FCC, 673 F.2d 1363 (D.C. Cir. 1982).

[79] See 18 U.S.C. § 2511(4).

"any measure taken by the organization to discipline any . . . employee . . . responsible for the offense and to prevent a recurrence of such an offense."[80]

U S WEST's existing policies are testament to the effectiveness of these incentives. U S WEST's internal security policies and procedures, as well as its corporate policies governing employee conduct, provide for discipline -- up to and including dismissal -- for employees who violate the law or company policy. U S WEST should be able to operate within this corporate structure without being required to report all violations of corporate policy to federal regulators or law enforcement agencies.

VII. CONCLUSION

It is appropriate for the Commission to begin developing the framework for CALEA implementation at this time. In doing so, it is critical that the Commission start out with the correct understanding of the jurisdictional scope of CALEA. That statute does not apply to the providers of information services, including enhanced services such as voice mail, regardless of whether the provider is an entity whose total business is dedicated to the exclusive provision of information services or is a entity with multiple lines of business (including common carrier operations). The Commission should so conclude.

Additionally, the framework for CALEA implementation should not include the kind of detailed prescription regarding internal carrier practices and policies that the NPRM suggests. Undoubtedly, many carriers currently have more than

---

[80] See id. § 3572(a)(8).

satisfactory internal policies regarding their interactions with law enforcement. Indeed, those practices probably include the vast majority of items/elements that the Commission proposes should be included in such policies. For this reason alone, a prescription of elements is unnecessary.

But beyond that, neither compliance regarding lawful interceptions nor the public interest require extensive federal regulatory insinuation into the matter of internal carrier practices and policies. As U S WEST demonstrates herein, we have never been a party to an unlawful interception. And, we believe that our historical experience is probably replicated many times over in the industry. Furthermore, our relationships with law enforcement are professional and cooperative. Therefore, a Commission prescription of elements to be included in our internal practices would not advance the public interest (i.e., by assuring greater protection of individual's rights or better cooperation/coordination with law enforcement).

U S WEST's proposal that the Commission adopt Guidelines, coupled with a streamlined certification process, is a far better framework for Section 229 implementation. Such a framework would provide necessary regulatory direction, for those carriers in need of such direction, and would substantially reduce the administrative burden associated with Commission approval of carrier policies. We urge the Commission to give serious consideration to such a framework.

Finally, the Commission should make clear to all CALEA-affected parties that, under the statutory provisions, compliance with CALEA is not now reasonably achievable. Indeed, the Commission should make clear that compliance will not be reasonably achievable at least until such time that carriers have network